UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/663,891	09/18/2000	Robert Chojnacki	N0064US	4137

37583 7590 03/03/2006

NAVTEQ NORTH AMERICA, LLC
222 MERCHANDISE MART
SUITE 900, PATENT DEPT.
CHICAGO, IL 60654

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/663,891	CHOJNACKI, ROBERT	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6 and 8-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 8-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/12-19-2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/19/2005 has been entered.

Response to Amendment

Applicant's arguments/amendments with respect to amended claims 1, 8, 10, & 24 and previously presented claims 2-6, 9, 11-23, & 25-39 filed 12/19/2006 have been fully considered and therefore the claims are rejected under new grounds.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1-6 and 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porter et al., United States Patent No. 5,845,067 and Hardy et al., United States Patent No. 5,623,546.

As per claim 1:

Porter et al. teach a method for on-line mass distribution of data products to end users, the method comprising: maintaining a first portion of each of said data products at a first location (col. 3, lines 28-34), maintaining a second portion of each of said data products at a second location (col. 3, lines 35-56); for each of said end users, confirming the end user's entitlement to one of said data products (col. 5, lines 30-35); obtaining a first portion of said one of said data products from said first location and a second portion of said one of said data products from said second location; combining said first portion of said one of said data products and said second portion of said one of said data products, and providing said combined first portion and second portion to said user (col. 1, lines 41-46).

Not explicitly disclosed by Porter et al. is wherein said step of combining is performed at said second location wherein second user is located at said second location. However, Hardy et al. teach that the client's portable device stores half of a key that is used to decrypt content where the first location stores the data and the other half of the key which are transferred to the client host for decryption of the data product with the corresponding product key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Porter et al. to combine the portions at the second location which is where the end user is located in order to receive the data they have been authorized to receive. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Hardy et al. suggest that split key encryption ensure key secrecy as well as allowing for data confidentiality so that only those authorized end users can obtain the data in col. 1, lines 19-39 and col. 2, lines 38-54.

As per claim 2:

Porter et al. and Hardy et al. substantially teach the method, as applied to claim 1 above. Not explicitly disclosed is the method, wherein said data products include geographic databases. However, Porter et al. teaches that a document can be any information stored as files in a file system, which can equate to the information contained by a geographic database. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Porter et al. for the data product to include files of geographical information stored in a file system, which is equivalent to a database. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Porter et al. in col. 7, lines 26-32.

As per claim 3:

Porter et al. and Hardy et al. substantially teach the method of claim 1. Furthermore, Porter et al. teach wherein said data products include digital copies of movies (col. 7, lines 27-32).

As per claim 4:

Porter et al. and Hardy et al. substantially teach the method of claim 1. Furthermore, Porter et al. teach wherein said data products include digital copies of musical songs (col. 7, lines 27-32).

As per claim 5:

Porter et al. and Hardy et al. substantially teach the method, as applied to claim 1 above. Furthermore, Hardy et al. teach the method further comprising the step of: encrypting said first portion of each of said data products (col. 3, line 66 – col. 4, line 13).

As per claim 6:

Porter et al. and Hardy et al. substantially teach the method, as applied to claim l above. Furthermore, Hardy et al. teach the method, further comprising the step of prior to the step of combining, encrypting said first portion of one of said data products (col. 3, line 66 – col. 4, line 13).

As per claim 8:

Porter et al. substantially teaches a system for secure on-line mass distribution of data products to end users comprising: an entity having associated therewith copies of first portions of a plurality of data products (col. 1, lines 27-33); a plurality of data distribution terminals, each of which has associated therewith copies of second portions of said plurality of data products (col. 1, lines 33-37); a communications system that provides for exchange of data between the entity and said plurality of data distribution terminals (fig. 3), and a data distribution program that provides copies of said data products to those end users who are entitled to have said copies thereof (col. 1, lines 38-46), wherein said data distribution program provides a copy of a data product by combining a copy of the first portion of said data product obtained from said authorization server with a copy of the second portion of said data product obtained from one of said plurality of data distribution terminals (col. 1, lines 38-46).

Not explicitly disclosed by Porter et al. is an "authorization server" as the entity. However, Porter et al. teach that the devices can be clients or servers. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Porter et al. to use an authorization server to hold the first portion of the plurality of data products. This modification would have been obvious because a person having ordinary

skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Porter et al. in col. 3, line 66 – col. 4, line 5.

Also not explicitly disclosed by Porter et al. is wherein said step of combining is performed at said second location wherein second user is located at said second location. However, Hardy et al. teach that the client's portable device stores half of a key that is used to decrypt content where the first location stores the data and the other half of the key which are transferred to the client host for decryption of the data product with the corresponding product key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Porter et al. to combine the portions at the second location which is where the end user is located in order to receive the data they have been authorized to receive. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Hardy et al. suggest that split key encryption ensure key secrecy as well as allowing for data confidentiality so that only those authorized end users can obtain the data in col. 1, lines 19-39 and col. 2, lines 38-54.

As per claim 9:

Porter et al. and Hardy et al. substantially teach the system, as applied to claim 8 above. Furthermore, Porter et al. teach wherein said authorization server also has associated therewith an authorization database containing data indicating entitlement by said end users to copies of said data products (fig. 1, element 120 and 130).

III. Claims 10-22, and 24-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porter et al., United States Patent No. 5,845,067 and Ginter et al., United States Patent No. 6,237,786.

As per claims 10 and 24:

Hardy et al. substantially teach a system/method comprising, in combination: a first entity maintaining the first portion (col. 2, lines 38-46); a second entity maintaining the second portion (col. 2, lines 38-46); a first set of logic executable by the first entity to encrypt the first portion so as to produce an encrypted first portion that can be decrypted using a first decryption key (col. 4, lines 45-60), wherein the first entity sends the encrypted first portion via a telecommunications link to the second entity (col. 5, lines 53 – col. 6, line 18); a second set of logic executable by the second entity, upon receipt of the encrypted first portion, to record onto the storage medium the encrypted first portion and the second portion wherein an end user of the data product is location at said second location where the encrypted first potion and the second portion are recorded onto the storage medium (col. 1, lines 19-39 and col. 2, lines 38-54).

Not explicitly disclosed is the third entity gaining access to the first decryption key in order to access the data product. However, Ginter et al. teach that in order for a third party, or any party for that matter, to gain access to the data product they must first have the appropriate decryption key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Porter et al. for a third entity to gain access to the first decryption key in order to access the data product. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was

made, would have been motivated to do so since it is suggested by Ginter et al. in col. 131, lines 18-44.

As per claims 11 and 25:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 10 and 24. Furthermore, Ginter et al. teach the method/system wherein the first entity sends to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product, and wherein the second set of logic is further executable to record onto the storage medium the encrypted authorization key (col. 14, lines 21-43 and col. 22, lines 13-45).

As per claims 12 and 26:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 11 and 25. Furthermore, Ginter et al. teach the method/system wherein the second decryption key is derived as a function of an environmental parameter (col. 22, lines 13-45).

As per claims 13 and 27:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 12 and 26. Furthermore, Ginter et al. teach the method/system wherein the environmental parameter comprises an identification code associated with the entity authorized to access the data product (col. 22, lines 13-45).

As per claims 14 and 28:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 11 and 27. Furthermore, Ginter et al. teach the method/system wherein the third entity

generating the second decryption key as the function of the identification code; the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and the third entity using the verification information to validate storage of the data product (col. 131, lines 18-44).

As per claims 15 and 29:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 11 and 25. Furthermore, Ginter et al. teach the method/system wherein a third set of logic executable by a third entity to decrypt the encrypted authorization information, to thereby gain access to verification information, and to compare at least a portion of the verification information to predetermined information associated with the third entity so as to determine whether the third entity is authorized to gain access to the data product (col. 131, lines 18-67).

As per claims 16 and 31:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 15 and 30. Furthermore, Ginter et al. teach the method/system wherein the predetermined information associated with the third entity comprises an identification code (col. 131, lines 40-44).

As per claims 17 and 30:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 10 and 29. Furthermore, Ginter et al. teach the method/system wherein the first entity sends to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information

indicative of an entity authorized to access the data product (col. 14, lines 21-43 and col. 22, lines 13-45).

As per claims 18 and 33:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 17 and 32. Furthermore, Ginter et al. teach the method/system wherein the second decryption key is derived as a function of an environmental parameter (col. 22, lines 13-25).

As per claims 19 and 34:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 18 and 33. Furthermore, Ginter et al. teach the method/system wherein the environmental parameter comprises an identification code associated with the entity authorized to store the data product (col. 22, lines 13-25).

As per claims 20 and 35:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 11 and 34. Furthermore, Ginter et al. teach the method/system wherein the third entity generating the second decryption key as the function of the identification code; the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and the third entity using the verification information to validate storage of the data product (col. 104, line 25 – col. 106, line 15).

As per claims 21 and 37:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 11 and 36. Furthermore, Ginter et al. teach the method/system wherein a third set of logic executable by a third entity to decrypt the encrypted authorization information, to thereby gain

access to verification information, and to compare at least a portion of the verification information to predetermined information associated with the storage medium so as to determine whether the storage medium is authorized to gain access to store the data product (col. 78, lines 8-58).

As per claims 22 and 38:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 21 and 37. Furthermore, Ginter et al. teach the method/system wherein the predetermined information associated with the storage medium comprises and identification code (col. 22, lines 13-45).

As per claim 32:

Hardy et al. and Ginter et al. substantially teach the method as applied to claim 24. Furthermore, Ginter et al. teach the method further comprising sending to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to store the data product (col. 14, lines 21-43 and col. 22, lines 13-45).

As per claim 36:

Hardy et al. and Ginter et al. substantially teach the method as applied to claim 32. Furthermore, Ginter et al. teach the method further comprising the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and the third entity using the verification information tot validate storage of the data product (col. 104, line 25 – col. 106, line 15).

IV. Claims 23 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardy et al., United States Patent No. 5,623,546 and Ginter et al., United States Patent No. 6,237,786 as applied to claims 10 and 24 above, and further in view of Ahrens et al., United States Patent No. 5,951,620.

As per claims 23 and 39:

Hardy et al. and Ginter et al. substantially teach the method/system as applied to claims 10 and 24. Not explicitly disclosed is the method/system wherein the third entity comprises a navigation system. However, Ahrens et al. teach the use of a navigation system. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Porter et al. for the third entity to be a navigation system. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ahrens et al. in col. 7, lines 29-44.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,308,179
2. US Patent No. 5,917,908
3. US Patent No. 6,204,774

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nadia Khoshnoodi
Examiner
Art Unit 2137
2/27/2006

NK

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER